Chapter 8: Troubleshooting your Authentication Problems

This chapter is intended to help users who are having trouble authenticating to Kerberos and logging in to Kerberized machines. We include information that should help you figure out what's causing your problem, and to fix it.

If you don't find the solution to your problem here, send mail to *kerberos-users@fnal.gov* requesting help in diagnosing the failure. Please include: principal name, date, time and IP address from which authentication failed, in addition to the error message and other error-related information.

- In many cases, when authentication fails, one of four things is likely to be wrong:
  - (1) your password,
  - (2) the date/time on your system (see section 14.1.7 *Synchronize your Machine with Time Server* for UNIX, 19.4 *Time Synchronization* for Windows, or 23.1.5 *Time Synchronization* for Mac OS X),
  - (3) the local host name in the `/etc/hosts` file (see section 16.3 *The /etc/hosts File*), or
  - (4) your CRYPTOCard is not configured for the target realm. The error message doesn't necessarily help you determine the problem: "`Preauthentication failed ...`", or "`Cannot establish a session with Kerberos administrative server...`" If this is the problem, bring your card to WH8NE to have it reprogrammed.

  For **WRQ** connections, click **HELP** for possible causes. It's usually a realm mismatch, a wrong password, or a system clock error.
- "Incorrect net address" usually refers to NAT (see section 6.5 *Network Address Translation*) or a multiple-IP address host. For UNIX, edit the `[libdefaults]` in `/etc/krb5.conf`: add `proxy_gateway=<your fixed IP address>`. For **WRQ**, there is no solution other than to change ISP or **WRQ** software. For Macintosh, edit the `[libdefaults]` in the Kerberos Preferences file: add `noaddresses=true`.
- YP problem: The error "`do_ypcall: clnt_call: RPC: Timed out`" typically indicates a local problem on your system or site network. Your machine is likely using YP (NIS) for host name-to-address resolution and you have a transient problem with your YP server(s).

- When using the Kerberized versions of **telnet**, **rlogin**, or **rsh** (see Chapter 13: *Network Programs Available on Kerberized Machines*) to connect to another machine in the strengthened realm, some users have had to use the **`-l <login_name>`** option even when the login names on both systems match. (Don't ask why.) You definitely need to use this option if the login names don't match.
- "KDC policy rejects request" or "KDC can't fulfill requested option" usually means either you're requesting a forwardable ticket for a /root or /admin instance of your principal (not allowed), or you're trying to forward a ticket that's not forwardable, or renew one that's not renewable.
- "Key version number for principal in key table is incorrect" means either the keytab has changed since the service ticket was obtained (to solve, run **`kinit -R`** or **`kinit`**), or the service key (for host principal) in the KDC was changed after the keytab file was created (to solve, recreate keytab file on host, see section 16.10 *Installing Service Host Keys*).
- "Cannot contact any KDC for requested realm." Caused by firewall blocking KDC request or reply, or DNS failure.
- "Server not found in Kerberos database" Possible causes include: local hosts file or NIS map giving wrong name for host (check `/etc/hosts` file and make sure the full official host name appears first, not a nickname; see section 16.3 *The /etc/hosts File*), or a bad or missing `[domain_realm]` mapping in `/etc/krb5.conf`. It was also a bug in Fermi Kerberos v1_2; to solve, upgrade.
- "aklog: Couldn't get fnal.gov AFS tickets:, aklog: unknown RPC error (-1765328352) while getting AFS tickets". You may have failed to get fresh tickets from your screensaver unlock. A fresh **`kinit`** should clear this right up.
- Syslog message: Principal <principalname>@FNAL.GOV ... for local user <user> failed krb5_kuserok. `krb5_kuserok` is a function in the kerberos library. It is accessed by krshd, and fails for these reasons:
  - · requested user has no account on target system
  - · `krb5_unparse_name` fails
  - · can't open `~user/.k5login`
  - · `~user/.k5login` not owned by user or root
  - · principal doesn't match any line in `.k5login` (try **`od -c ~user/.k5login`** to look for any "invisible" characters in this file).
- If Kerberos functions are very slow on a client host, check its Kerberos logs for long intervals between "NEEDED_PREAUTH" and "ISSUE" and see if there are few or no repeats of the same request to different KDCs. If so, the client host's first-configured DNS server may be slow or dead.

To resolve this, check the DNS server list (`/etc/resolv.conf` on UNIX-like systems, Network Control Panel on Windows) and test each one, moving dead servers down in the list or removing them.

SSH Problems

- Make sure the instance of the **ssh** product you're using matches the OS version of your target UNIX machine.
- When you use the Kerberos-aware ssh or scp client (v1_2_27f) to connect to a node that's running a non-Kerberos-aware sshd, the client ignores a `.shost` file on the remote node. It tries Kerberos, that of course fails, then it prompts for a password. Supplying the password works. (This is an unavoidable side-effect.)
- Some users of Kerberized **ssh** v1_2_27 have encountered a harmless but misleading message upon authentication:

  ```
  aklog: can't get afs configuration
  (afsconf_Open(/usr/vice/etc))
  ```

  To get rid of this message, add `AFSRunAklog no` to `/etc/sshd_config` and restart **sshd**.
- Logins from Kerberized **ssh** clients to unstrengthened **ssh** servers can fail. This does not happen with the Fermi **ssh**. You can work around this by explicitly using the **`-l <login_name>`** option even if the login names on both systems match. (Again, don't ask why.)
- If you get prompted for a password when you login from a machine with Kerberized ssh, and you already have valid tickets, check to make sure the following line is in the `[domain_realm]` section of your `/etc/krb5.conf` file:

  ```
  .fnal.gov = FNAL.GOV
  ```

  Kerberized ssh token-passing won't work without it, nor will FTP.